UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/817,275	04/01/2004	Michael A. Horwitz	16010-07728	2281

758 7590 04/21/2008

FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
SAN JUAN, MARTINJERIKO P	
ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
04/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/817,275	HORWITZ ET AL.	
	Examiner	Art Unit	
	MARTIN JERIKO P. SAN JUAN	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 April 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/24/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This is a response to Applicant's Amendments filed on February 1, 2008.

Claims 1-29 were originally pending.

Claims 1-29 were rejected on May 16, 2007.

Claim 14 was amended.

Claims 1-29 were rejected on October 24, 2007.

Claims 1, 3-5, 7, 11, 12, 14-16, 18, 19, and 24 have been amended.

Claims 1-29 are currently pending.

Response to Arguments

1. Applicant's arguments filed January 24, 2008 have been fully considered but they are not persuasive.

Applicant argues Roberts does not teach "a plurality of independent local applications." Server-provided applets constitute neither "independent" nor "local" applications, as claimed. Rather, they exist solely for the purpose of communicating with the other downloaded applet.

The Examiner respectfully disagrees. Even as amended, Roberts still teaches "a plurality of independent local applications" [US 6295551 B1, Col 3, Ln 26-30]. A browser type application reads on independent and local applications. A browser

application is independent because it can run by itself, and it is local because it is installed on every platform terminal. The applets exist solely for the purpose of communicating data associated with the browser application to/from a server and other terminal platforms. Note that Applicant's Specification on Fig 2B shows a browser type application on machine 220d. This is also supported on Applicant's Specification on Par. 0041. The Examiner notes that the browser running web applications communicates both authentication and non-authentication data through the use of the applets. The Examiner notes that any data communicated between browsers running web applications read on either authentication or non-authentication data.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

1. Claim 1-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roberts et al. [US 6295551 B1] hereinafter Roberts, and further in view of Satyavolu et al. [US 7225464 B2] hereinafter Satyavolu.

Regarding claim 18, Roberts teaches a method of sharing data across a computing system, the method comprising: receiving requests to authenticate the authenticated user from a plurality of independent local applications [US 6295551 B1, Col 3, Ln 26-30] on a plurality of computing platforms being accessed by the authenticated user [US

6295551 B1, Col 11, Ln 14-15]; receiving non-authentication data provided by a first instance of the authenticated user using a local application in a first domain [US 6295551 B1, Col 8, Ln 23-26]; storing in a data registry the non-authentication data provided by the first instance of the authenticated user using the local application in the first domain [*It is inherent that non-authentication data has been stored if each computers are retrieving the shared content independently*. US 6295551 B1, Col 8, Ln 35-40]; receiving a request for non-authentication data from a second instance of the local application in a second domain [US 6295551 B1, Col 8, Ln 1-11], and supplying, from the data registry, the requested non-authentication data provided by the first instance of the local application in the first domain to the second instance of the local application in the second domain [US 6295551 B1, Col 8, Ln 25-26].

Roberts does not explicitly teach receiving requests subsequent to an initial authentication of a user and automatically authenticating the authenticated user to the plurality of independent local applications being accessed by the authenticated user responsive to the initial authentication of the user.

Satyavolu teaches receiving requests subsequent to an initial authentication of a user [US 7225464 B2, Col 6, Ln 30-32] and automatically authenticating the authenticated user to the plurality of independent local applications being accessed by the authenticated user responsive to the initial authentication of the user [US 7225464 B2, Col 6, Ln 54-62].

It would have been obvious to one of ordinary person skilled in the art at the time of invention to include SSO or Single Sign On architecture of Satyavolu to the invention of Roberts. The suggestion/motivation for including SSO is to enable the user to avoid repeated login procedures [US 7225464 B2, Col 2, Ln 1-5]. Satyavolu is analogous art because it solves the problem of users of avoiding repeated login procedures for accessing applications/resources across different terminals/platforms.

Regarding claim 19, Roberts and Satyavolu teach the method of claim 18, wherein the second instance of the local application in the second domain is associated with a second user [US 6295551 B1, Col 13, Ln 61].

Regarding claim 20, Roberts and Satyavolu teach the method of claim 18, further comprising: receiving log on information from a user [US 7225464 B2, Col 2, Ln 1-5]; determining that the user is logging on to the computing system for the first time [US 7225464 B2, Col 6, Ln 11-13]; subsequent to the determination that a user is logging on to the computing system for the first time, verifying the identity of the user [US 7225464 B2, Col 6, Ln 1]; prompting the user to supply a user id and password [US 7225464 B2, Col 6, Ln 2]; providing the user id and password supplied by the user to a data registry to be stored therein [US 7225464 B2, Col 2, Ln 20-23]; capturing application authentication information provided by the user during the computing session [US 7225464 B2, Col 2, Ln 55]; storing the application authentication information provided

by the user during the computing session in the data registry [US 7225464 B2, Col 2, Ln 45-46] wherein the data registry is configured to store authentication and non-authentication data [US 6295551 B1, Col 14, Ln 48-59].

Regarding claim 21, Roberts and Satyavolu teach the method of claim 18, wherein an operating platform used by the first domain differs from an operating platform used by the second domain [*Operating platform used by the first domain differs from an operating platform used by the second domain is taught since JAVA objects are being utilized enabling a "cross-platform" system. US 6295551 B1, Col 8, Ln 52-65*].

Regarding claim 22, Roberts and Satyavolu teach the method of claim 18, further comprising storing authentication data in the data registry [US 6295551 B1, Col 14, Ln 55-56] [US 7225464 B2, Col 2, Ln 45-46].

Regarding claim 23, Roberts and Satyavolu teach the method of claim 18, wherein the non-authentication data provided by the first instance of the local application in the first domain comprises configuration information for customizing a user's application environment [US 6295551 B1, Col 12, Ln 66 – Col 13, Ln 60].

Regarding claim 24, Roberts and Satyavolu teach the method of claim 18, wherein the non-authentication data provided by the first instance of the local application in the first domain includes state information with which the user's application state from the first

instance of the local application in the first domain can be maintained to the second instance of the local application in the second domain [US 6295551 B1, Col 12, Ln 66 – Col 13, Ln 60] [US 6295551 B1, Col 14, Ln 48-59] [US 6295551 B1, Col 18, Ln 35-38].

Regarding claim 25, Roberts and Satyavolu teach the method of claim 18, wherein storing the non-authentication data comprises: configuring a non-authentication data attribute; storing a value for the non-authentication data attribute associated with the user; and responsive to a request identifying the non-authentication data attribute, providing the value of the non-authentication data attribute to a requesting application [US 6295551 B1, Col 12, Ln 66 – Col 13, Ln 60] [US 6295551 B1, Col 14, Ln 48-59] [US 6295551 B1, Col 18, Ln 35-38].

Regarding claim 26, Roberts and Satyavolu teach the method of claim 18, wherein the request for non-authentication data associated with the authenticated user is generated responsive to a call trigger [US 659551 B1, Col 8, Ln 45-51].

Regarding claim 27, Roberts and Satyavolu teach the method of claim 18, wherein the step of receiving non-authentication data provided by a first instance of an application used by the authenticated user comprises receiving the non-authentication data from a synchronizing module on a computer for sending non-authentication data from the local cache of the computer, the data having been stored in the local cache when the

authenticated user was disconnected from the networked system [US 659551 B1, Col 9, Ln 25-38].

Claim 1 is rejected because it is the system apparatus performing the method of claim 18.

Regarding claim 2, Roberts and Satyavolu teach the cross-platform single sign-on system of claim 1, wherein web services technologies are used to transmit requests for authentication and non-authentication data from a plurality of computer systems hosting the plurality of applications to the interface module [US 6295551 B1, Col 8, Ln 52-65] [US 7225464 B2, Col 5, Ln 41 -- XML].

Regarding claim 3, Roberts and Satyavolu teach the cross-platform single sign-on system of claim 1, wherein the non- authentication data includes state information reflecting a state of a selected local application on a first computer accessed by the user that can be retrieved when the selected local application is being accessed from a second computer [US 6295551 B1, Col 12, Ln 66 – Col 13, Ln 60] [US 6295551 B1, Col 14, Ln 48-59] [US 6295551 B1, Col 18, Ln 35-38] [*For different browsers showing identical/synchronous information, it is inherent that state information is being transferred.*].

Claim 4 is rejected because it is the system apparatus performing the method of claim 19.

Regarding claim 5, Roberts and Satyavolu teach the cross-platform single sign-on system of claim 1, wherein the interface module is further configured to receive requests to store authentication and non- authentication data associated with the user from a plurality of independent local applications on a plurality of computing platforms in the computing system and, based upon authentication of a user at the beginning of a computing session and responsive to the requests, to store the data to the data registry [*Non-authentication data, eg. state information, has been stored by the server if the server needs to wait for an acknowledgement for the shared content to be updated.* US 6295551 B1, Col 8, Ln 25-26] [US 7225464 B2, Col 2, Ln 45-46].

Regarding claim 6, Roberts and Satyavolu teach the cross-platform single sign-on system of claim 1, wherein the interface module formats data queries to the data registry in accordance with a data exchange protocol accepted by the data registry [US 7225464 B2, Col 5, Ln 39-59] [J*avascript* – US 6295551 B1, Col 12, Ln 60].

Regarding claim 7, Roberts and Satyavolu teach the cross-platform single sign-on system of claim 1, wherein the data registry is further configured to receive requests for authentication and non-authentication data directly from the plurality of independent

local applications on the plurality of computing platforms, and for the requested data to be retrieved from the data registry responsive to the requests [US 629551 B1, Col 12, Ln 39-50] [US 6295551 B1, Col 14, Ln 48-59] [*The data registry is hosted in the server and thus receive requests directly from other computers requesting a connection/session. The passage teaches the many different kinds of authentication and non-authentication data being transferred.*] [US 7225464 B2, Col 2, Ln 45-46].

Regarding claim 8, Roberts and Satyavolu teach the cross-platform single sign-on system of claim 1, wherein a request to retrieve authentication and non-authentication data associated with the user is sent responsive to an event trigger activated during the user's computing session [US 6295551 B1, Col 8, Ln 45-51].

Regarding claim 9, Roberts and Satyavolu teach the cross-platform single sign-on system of claim 8, wherein the event trigger comprises at least one of: the authentication of a user, a user command, and the passage of a pre-determined interval of time [US 6295551 B1, Col 8, Ln 1-17].

Regarding claim 10, Roberts and Satyavolu teach the cross-platform single sign-on system of claim 1, wherein the interface module and authentication module are commonly hosted on a single computer [US 7225464 B2, Fig 1].

Regarding claim 11, Roberts and Satyavolu teach the cross-platform single sign-on

system of claim 1, wherein at least one of the plurality of computing platforms differs from at least another of the plurality of computing platforms [*An operating platform used by the first domain differs from an operating platform used by the second domain is taught since JAVA objects are being utilized enabling a "cross-platform" system.* US 6295551 B1, Col 8, Ln 52-65].

Regarding claim 12, Roberts and Satyavolu teach the cross-platform single sign-on system of claim 1, further comprising: a caching module for storing non-authentication data generated by an application in the local cache of the computer hosting the local application when the computer is disconnected from the computing system; and a synchronizing module for sending non-authentication data stored in the local cache to the data registry when the computer is connected to the computing system [US 6295551 B1, Col 9, Ln 25-38 --*The "persistent" applet is loaded into a local cache and being persistent inherently teaches a synchronizing module that will keep computers in-synchronization as long as the computer remains in a session. It inherently teaches protecting sessions from network interruptions since it explicitly states that it remains in the cache unless it gets removed by the user computer.*].

Claim 13 is rejected because it is the system apparatus performing the method of claim 20.

Regarding claim 14, Roberts and Satyavolu teach a data registry for storing and providing data across a computing system, the data registry comprising [*There is implementation of database/data registry.* US 6295551 B1, Col 11, Ln 27]: a plurality of user data entries [US 6295551 B1, Col 11, Ln 25-31], each of the user data entries describing a unique user of a computing system comprised of a plurality of computing platforms and a plurality of independent local applications [*There exist different types of users with different kinds of roles, and types of computer, ie. sales representative, customer, administrator.* US 6295551 B1, (Col 11, Ln 5) (Col 10, Ln 57)]; a plurality of authentication entries associated with each of the user data entries for authenticating the user on the plurality of independent local applications of the computing system [US 6295551 B1, Col 11, Ln 5-14 -- *This passage inherently teach a plurality of authentication entries because the server can ascertain and validate which type of user is making a request.*]; and a plurality of non-authentication attributes and attribute entries associated with each of the user data entries in which information about a user's use of a local application can be preserved [US 6295551 B1, Col 10, Ln 56-67; Col 14, Ln 48-59 -- *Passage inherently teach a plurality of non-authentication attributes and attribute entries because the server can ascertain what applet and associated objects are needed by the local browser from a user making the request. Also the passage teaches a session box which inherently capture information about a user's use of an application.*].

Regarding claim 15, Roberts and Satyavolu teach the data registry of claim 14, wherein the non-authentication data includes state information for one of the plurality of independent local applications, whereby a user may switch between a first computer and a second computer and preserve the state of a selected application accessed using the first computer when accessing the selected application from the second computer [US 6295551 B1, Col 12, Ln 66 – Col 13, Ln 60; Col 14, Ln 48-59; Col 18, Ln 35-38].

Regarding claim 16, Roberts and Satyavolu teach the data registry of claim 14, wherein the non-authentication data includes configuration information for one of the plurality of independent local applications with which a user's application environment can be customized [US 6295551 B1, Col 12, Ln 66 – Col 13, Ln 60].

Regarding claim 17, Roberts and Satyavolu teach the data registry of claim 14, further comprising an interface module that receives web service requests for storing and providing data from one of the plurality of independent local applications and, responsive to the requests, saves the data to the data registry [US 6295551 B1, Col 12, Ln 39-50 -- *The data registry is in the server that also runs the applet associated with the local browser. This passage cites command scripts which teaches web service requests.*]

Regarding claim 28, Roberts and Satyavolu teach the system of claim 1, wherein the non-authentication data comprises one of: configurations data, settings data, or

applications data, environment data [US 659551 B1, Col 12, Ln 66 – Col 13, Ln 60] [US 659551 B1, Col 14, Ln 48-59] [US 659551 B1, Col 18, Ln 35-38].

Regarding claim 29, Roberts and Satyavolu teach the system of claim 1, wherein the non-authentication data comprises one of: a size of a window, the configuration of a tool bar, and the selection of open files [US 659551 B1, Col 12, Ln 66 – Col 13, Ln 60] [US 659551 B1, Col 14, Ln 48-59] [US 659551 B1, Col 18, Ln 35-38].

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARTIN JERIKO P. SAN JUAN whose telephone number is (571)272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/
Martin Jeriko San Juan
Examiner. Art Unit 2132.

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132